

## UNITED STATES DISTRICT COURT

for the  
Middle District of North Carolina

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
Cameron James Brown, DOB 6/10/2000

Case No. 1:21MJ 403 -1

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Cameron James BROWN, as further described in Attachment B

located in the Middle District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

Evidence of, instrumentalities used in committing, and fruits of the crimes pertaining to violations of 18 U.S.C. Section 2252A, as further described in Attachment C.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252A(a)(2)(A)	Receipt/Distribution of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:  
See attached affidavit incorporated by reference herein

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/S/ Zachary M. Neeffe

Applicant's signature

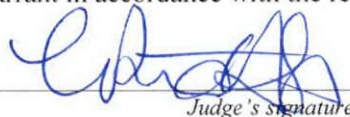
Zachary M. Neeffe, Special Agent - H.S.I.

Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date:

10/15/21

  
Judge's signature

City and state: Greensboro, North Carolina

L. Patrick Auld, U.S. Magistrate Judge

Printed name and title

## ATTACHMENT A

### *(Description of Property to be Searched)*

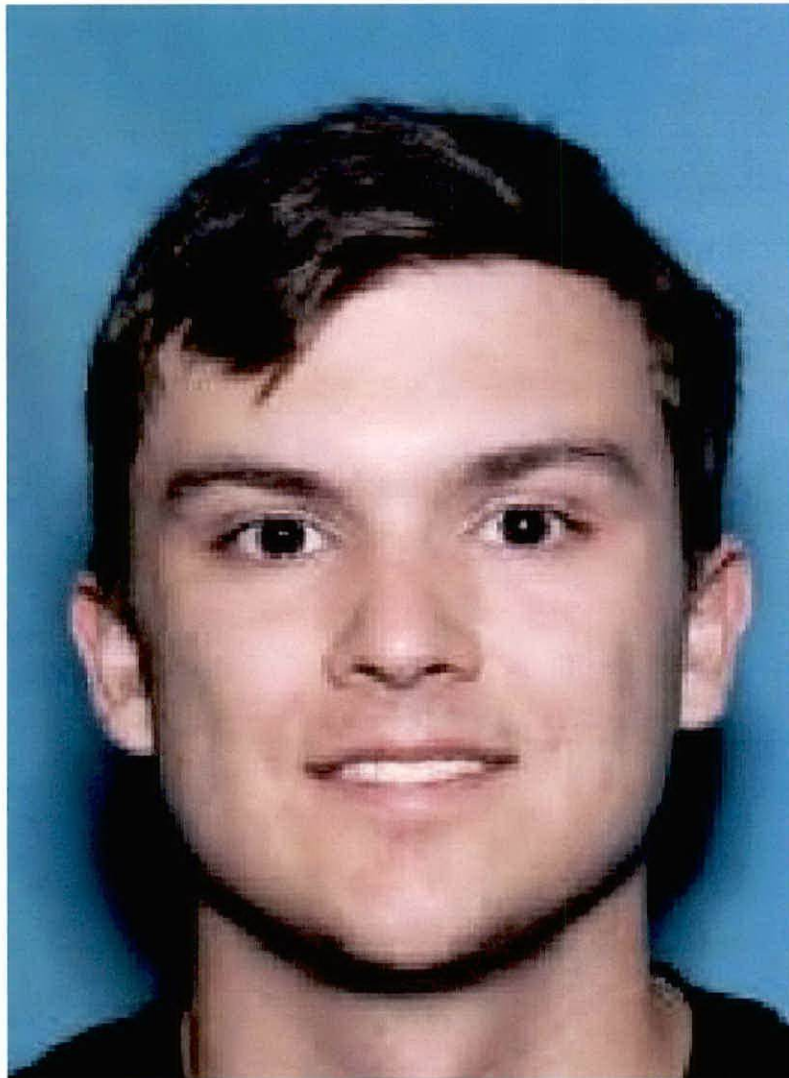
The entire property located at 6239 Keithgayle Drive Clemmons, North Carolina 27012, including the residence, any outbuildings, other structures and/or vehicles within the property's curtilage, and any appurtenances thereto (all which constitute the SUBJECT PREMISES). Local law enforcement and/or task force officers would be utilized in order to ensure execution of the search warrant at the correct physical location. This search would include computers and storage media found therein.





**ATTACHMENT B**

*(Person to be Searched)*



Cameron James BROWN, depicted above

DOB: 06/10/2000

**ATTACHMENT C**  
*(Items to be Seized)*

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 2252A:

1. Computers or storage media that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored, which may then be searched for the items set out below.
2. Routers, modems, and network equipment used to connect computers to the Internet.
3. Child pornography and child erotica.
4. Records and information relating to violations of the statutes described above in the form of:
  - a. Records and information referencing or revealing the occupancy or ownership of the SUBJECT PREMISES, 6239 Keithgayle Drive Clemmons, NC 27012;

- b. Records and information referencing or revealing the use or ownership of Kik user “cjb1298”, camjbrown1298@gmail.com, and/or the Verizon phone associated with telephone number: 336-341-5807;
- c. Records and information referencing or revealing the use of mobile messaging platform Kik;
- d. Records and information referencing or revealing the distribution, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;
- e. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence;
- f. Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved and location of occurrence;
- g. Records and information referencing or revealing participation in groups or the use of services that are known to be used to facilitate the distribution and/or storage of child pornography;
- h. Records and information referencing or revealing the use of remote computing services such as email accounts or cloud storage.

5. For any computer or storage medium whose seizure is otherwise authorized by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, deleted, viewed, or otherwise interacted with;
- b. evidence of how and when the COMPUTER was used to create, edit, delete, view, or otherwise interact with or engage in the things described in this warrant;
- c. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- d. evidence of the Internet Protocol addresses used by the COMPUTER;
- e. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- f. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- g. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- h. evidence of the lack of such malicious software;
  - i. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
6. During the course of the search, photographs of the location to be searched may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, smartphones, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives,

flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, to minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

- a. “Surveying” various file directories and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files).



- b. "Opening" or cursorily reading the first few pages of such files in order to determine their precise contents.
- c. "Scanning" storage areas to discover and possibly recover recently deleted files.
- d. "Scanning" storage areas for deliberately hidden files.
- e. Performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of child pornography or other criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH**  
**WARRANT**

I, Zachary M. Neefe, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I am investigating offenses related to child sexual exploitation. This Affidavit is submitted in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the premises located at 6239 Keithgayle Drive Clemmons North Carolina 27012 (the "SUBJECT PREMISES"), more specifically described in Attachment A and the person of Cameron James BROWN ("SUBJECT PERSON"), more specifically described in Attachment B, for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B), which are more specifically described in Attachment C.

2. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§

2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located at the SUBJECT PREMISES and/or on the person of BROWN.

### **AFFIANT BACKGROUND**

3. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI") since February of 2020 and am currently assigned to the Winston-Salem, North Carolina, Office of the Resident Agent in Charge. Prior to working with HSI, I was a detective and federal task force officer at the Alamance County Sheriff's Office in North Carolina where I specialized in child exploitation and sexual abuse investigations.

4. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training facilitated by the Internet Crimes Against Children ("ICAC") Task Force, at the National Cybercrimes Center ("C3"), and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography, child exploitation, and sex trafficking and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. My training through C3 and the ICAC Task Force has included undercover chats for child exploitation cases, peer-to-peer file sharing of child

pornography, online ads pertaining to enticement of children, and training specific to the Bittorrent file sharing technology. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 2252A (relating to child pornography), and I am authorized by law to request a search warrant.

### **STATUTORY AUTHORITY**

5. As noted above, this investigation concerns alleged violations of the following:

- a. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
- b. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of



child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

#### **DEFINITIONS**

6. The following definitions apply to this Affidavit and Attachment C:

- a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.
- b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct,

where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. Child pornography is also referred to as “child sex abuse material” or “CSAM” and has the same definition.

- c. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).
- d. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer

hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

- e. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot”

keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- f. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

- g. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.
- h. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- i. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
- j. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.
- k. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural,



and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

- l. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.
- m. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- n. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

### **PROBABLE CAUSE**

*Homeland Security Investigations Portland Initiates an Undercover Operation*

7. On May 5, 2021, Homeland Security Investigations (HSI) Portland executed a federal search warrant in Salem, Oregon related to the distribution of child pornography via Kik messenger<sup>1</sup>. This search warrant was signed by the Honorable Jolie A. Russo and was assigned case number 21-MC-528. The user of the Kik account admitted to the distribution of child sexual abuse material (CSAM)<sup>2</sup> and admitted that he was an administrator over several private group chats dedicated to the distribution of CSAM. The user subsequently signed over his online presence to HSI for further investigative activity. HSI Special Agent (SA) Clint Lindsly then maintained and controlled the Kik messenger account in an undercover capacity.

8. After assuming the user's online presence, SA Lindsly learned that there were approximately five (5) private group chats dedicated to the

---

<sup>1</sup> Kik Messenger is a free instant messaging and social networking app, now owned by the California based MediaLab, that uses a smartphone's data plan or Wi-Fi connection to send messages to other Kik users, bypassing SMS (short message service, aka text messaging). It's available on iOS, Android, and Amazon for Kindle Fire. While Kik is not unique in how it transmits communications, it differentiates itself with a distinctive but controversial effort to target a specific demographic: Kik appeals to the teenage crowd because of its emphasis on privacy and anonymity. As of 2016, Kik Messenger had some 300 million registered users and was used by an estimated 40% of teenagers in the U.S. It hasn't disclosed any user figures since 2016. (Footnote text based on digitaltrends.com article)

<sup>2</sup> By accepted best practice, the term "child pornography" will hereafter be referred to in this affidavit as "child sexual abuse material" or CSAM, which law enforcement and survivors agree better reflects the gravity of this criminal offense.

distribution of CSAM. SA Lindsly learned that Kik users were admitted by invite only and there was one master administrator and several sub administrators. The master administrator and sub administrators routinely posted CSAM in these private group chats and shared encrypted hyperlinks that contained CSAM. These Kik users were initially recruited from other “public” groups created by the master administrator that emphasized the distribution of CSAM. Since then, the “private” groups changed naming conventions on several occasions and were reduced to three groups<sup>3</sup>.

9. In SA Lindsly’s assumed role as administrator, not only did he learn how individuals came to be a part of the private groups, but he also learned how the groups and group chats work. At any point in time, any Kik user can view what other Kik users are in each private group chat. Each user can see every other user’s Kik profile picture and their username. Additionally, each Kik user can see which users are designated as the “administrator,” which is designated as either an orange circle with a picture of a crown, or a green circle with a picture of a crown. The user designated with the green circle and a picture of a crown is the chatroom’s master administrator / creator. The users

---

<sup>3</sup> As mentioned above, Kik has instant messaging features between individual users (called direct messaging or DMs within the app) as well as group messaging available in both public groups or private groups. The public groups can be joined by any user within the Kik application by scanning a QR code, accessing the group via a hyperlink in-app, or by keyword-searching for the group’s name. Private groups are accessible in-app by invite only.

designated with the orange circle with a picture of a crown are sub-administrators. Each chatroom has one master administrator/creator and a few sub-administrators. During the time that SA Lindsly was acting as an administrator, that number varied, between three to five. Each chatroom had a maximum of 100 users and usually had approximately 75 – 100 users at any given point in time.

10. SA Lindsly learned that there was a private group chat for the administrators only. SA Lindsly was added to this private administrator-only group chat and participated in conversations with other administrators. This chat was focused on managing the private group chats, flagging various users for violating the “rules,” and discussions about ways to avoid detection by law enforcement<sup>4</sup>. SA Lindsly also learned that the master administrator promoted other Kik users to sub administrators based on their activity level in the private group chats (i.e. they posted a lot of CSAM).

11. Each private group had “rules.” These rules included that anyone admitted to the chat rooms had to post child pornography upon entering or some other sex video; that each Kik user could be in only one chatroom at a time; and that private sharing among users was prohibited (i.e. everything had

---

<sup>4</sup> Although Kik supposedly reports illegal content to U.S. law enforcement, it has been well-documented that illegal activity, including distribution/receipt of CSAM, occurs regularly on this platform, making it easy for bad actors to avoid detection with basic obfuscation techniques.

to be posted in the group chat). Additionally, users would be removed from the private group chats for inactivity and violating the above rules. These rules were enforced by the main administrator and the sub administrators. Because of the role he had assumed as an administrator, SA Lindsly enforced these rules.

12. SA Lindsly has become familiar with the purpose of the chatroom that he assumed administrator responsibilities over by actively participating in and monitoring the chats that occurred therein. SA Lindsly has observed the distribution of hundreds of images and videos meeting the federal definition of child pornography within these chats. SA Lindsly has directly communicated with the master administrator and other sub administrators about the distribution of child pornography and managing / creating the group chats, wherein child pornography could be distributed. SA Lindsly has communicated with the master administrator about the purpose of the chats, which was the distribution of child pornography. Per HSI and Internet Crimes Against Children (ICAC) standards, SA Lindsly did not distribute child pornography in his role as a “sub administrator.”

13. Due to the high level of activity in these private group chats, the digital chat logs stored on an undercover computer/digital device will overwrite and/or are destroyed after approximately one to two calendar days. However,



investigators attempted to video record and document as much as possible, including downloading the media files that appeared to be child pornography.

14. In addition to posting images and videos of child pornography, some users entered the chatroom and boasted about sexually abusing their own children or having access to children. Using these leads, to date, investigators have identified and rescued over ten (10) children in the United States and Australia from sexual abuse.

15. In May and into early June 2021, the master administrator created several new groups and/or changed the group's naming conventions. In each instance of creating new groups, the names were changed but the administrator maintained the same three or four "tier" level structure. The master administrator maintained the public groups as the primary feeders to private groups. The public groups did not change until the end of May because one of the master administrator's secondary accounts was banned. However, investigators observed that banning of one group would merely result in another one popping up in its place.

16. The master administrator was arrested by HSI in the United States on June 3, 2021. However, even in the master administrator's absence, with the assistance of other sub administrators, the groups remained active until banned by Kik messenger on June 30, 2021. SA Lindsly's undercover accounts were also banned by Kik messenger.

*Kik User “cjb1298” Developed as Suspect in Clemmons, NC*

17. While controlling the undercover Kik account, SA Lindsly observed the Kik user “cjb1298”<sup>5</sup> in the private group chats. It is unclear when exactly the Kik user “cjb1298” was admitted. However, SA Lindsly observed the Kik user “cjb1298” post images and/or videos that met the federal definition of child pornography on at least the following dates: 5/17/21, 5/18/21, and 5/21/21. Investigators screen recorded the posting of the media files and downloaded the media files as evidence.

18. On May 21, 2021, SA Lindsly served a preservation request on Kik for the user “cjb1298.” SA Lindsly followed up the preservation request with an administrative subpoena for the user’s subscriber records. Eventually, Kik provided subscriber records and IP connectivity logs for the Kik user “cjb1298” which reflected the following:

- a. First Name: Cj
- b. Last Name: B
- c. Email: camjbrown1298@gmail.com
- d. Registration Timestamp: Unknown

---

<sup>5</sup> Kik users have two names by which they are identified within the platform. The name quoted above “cjb1298” is the permanent username for this user, accessible within app by clicking on the user’s profile and viewing additional details. The more prominent “vanity name” which is displayed on a user’s profile without the additional step of clicking for more details, is not a unique identifier and can be changed by a user at any time.

e. Device Type: iPhone

f. Date of Birth: March 20, 1999

19. In addition to the above information, Kik provided IP connectivity logs between May 13 and 31, 2021. During the review, SA Lindsly identified that the account “cjb1298” was accessed from various IP addresses resolving to Verizon Wireless (consistent with the use of a cell phone) and 24.163.8.3, which is serviced by Charter Communications.

20. SA Lindsly followed up by serving an administrative subpoena on Charter Communications for subscriber records related to IP address 24.163.8.3.

21. On June 17, 2021, Charter Communications provided a response to the aforementioned subpoena. According to the review of records, SA Lindsly learned that IP address 24.163.8.3 had the following subscriber information:

a. Subscriber Name: Denise Brown

b. Service Address: 6239 Keithgayle Drive, Clemmons, NC  
27012

c. Phone Number: 336-403-0223

d. Start of Lease: May 30, 2020

22. Utilizing law enforcement databases to include current North Carolina Division of Motor Vehicles records, SA Lindsly identified the following potential occupants at 6239 Keithgayle Drive, Clemmons, NC 27012:

- a. Denise Brown, date of birth January of 1972, with a specified NC Driver's License number, and no identifiable criminal history
- b. Cameron James BROWN, date of birth June 10, 2000, with a specified NC Driver's License number and no identifiable criminal history

23. Due to the IP address being used to access the Kik account "cjb1298" appearing to originate in the greater Winston Salem, NC area, HSI Portland referred this investigation for further follow up to HSI Winston-Salem SA Zachary Neeffe (the affiant).

*Additional Investigative Steps to Identify "cjb1298"*

24. After receiving the evidentiary files and investigative lead from HSI Portland, I requested and subsequently served an administrative subpoena on the Google account associated with camjbrown1298@gmail.com. Google returned subscriber information on July 27, 2021 as follows:

- a. Google Account ID: 853400059212
- b. Name: Cam Brown
- c. Given Name: Cam
- d. Family Name: Brown
- e. e-Mail: camjbrown1298@gmail.com
- f. Alternate E-Mails: [None Provided]

- g. Account Created On: 2019-11-28 03:33:57 UTC
- h. Recovery Email: Camjbrown2000@gmail.com
- i. Recovery SMS (text message by phone): +13363415807 [US]

25. Next, I requested and subsequently served an administrative subpoena on Verizon for the natted IP addresses<sup>6</sup> with ports associated with the “cjb1298” user on SA Lindsly’s Kik records return. Verizon returned subscriber information on August 2, 2021 as follows:

- a. Associated Telephone Number for Account: 3363415807
- b. Mobile Telephone Number (MTN) Status: Active
- c. MTN Status Effective Date: 12/15/2012
- d. Disconnect Date: [None Provided]
- e. Account Number: 723777618-1
- f. Last Name: Brown
- g. First Name: Denise
- h. Address: 6239 KEITHGAYLE DR
- i. City/State/Zip: CLEMMONS, NC 270129459

*Review of Evidentiary Files Provided by HSI Portland*

---

<sup>6</sup> Natting technology allows wireless carriers, in this case Verizon Wireless, to have multiple users utilizing the same IP address at the same time; for this reason, in order to learn the end-subscriber for a natted IP as in this case, process served on Verizon had to include not only the IP address and exact date/time used, but also the port used. The port serves as an additional routing mechanism for the Internet Service Provider, functioning in a similar manner as an additional address line would be utilized by a mail carrier.



26. Additionally, I reviewed the evidentiary files provided by SA Lindsly. The following statements within this affidavit are based on my personal observations from the evidentiary files provided to me by HSI Portland SA Lindsly:

27. On May 17, 2021, at approximately 12:40 AM (based on timestamps provided within the Kik application), the user cjb1298 shared three (3) embedded videos within the Gold Group 1 feed.

- a. The first video is 1 minute 56 seconds long. It shows the faces of three female prepubescent to pubescent minors at the beginning with caption "Sweet release...girls getting showered in CUM" the video then progresses to show numerous prepubescent to pubescent minor females (three at a time across the frame) with adult male penises present and ejaculating on the female minors' faces.
- b. The second video is 15 seconds long. It shows a pubescent (age-difficult) female stripping nude in a bathroom while lewdly/lasciviously displaying her genitals.
- c. The third video is 55 seconds long. It shows a pubescent (age-difficult) female stripping nude in a bedroom while lewdly/lasciviously displaying her genitals.

28. On May 18, 2021, at approximately 11:28 PM (based on timestamps provided within the Kik application), the user cjb1298 shared two (2) embedded videos within the Gold Group 1 feed.

- a. The first video is 1 minute and 5 seconds long. It depicts an adult male having penile/anal sex with a nude, pre-pubescent minor female. The male pinches the minor's labia with his fingers as he penetrates her with his penis. There are close-ups of the minor's genitals throughout and her face is visible at the end of the video.
- b. The second video is 26 seconds long. It depicts an adult male having penile/vaginal sex with a pre-pubescent minor female, who is only wearing a shirt.

29. On May 19, 2021 at approximately 11:04 PM (based on timestamps provided within the Kik application), the user cjb1298 shared one (1) embedded video within the Gold Group 1 feed.

- a. The video is 49 seconds long. It shows a pubescent (age difficult) female laying apparently asleep on a bed, then having her face ejaculated on by an adult male.

30. On May 21, 2021 at approximately 10:16 PM (based on timestamps provided within the Kik application), the user cjb1298 shared two (2) embedded videos within the Gold Group 1 feed.

- a. The first video is 1 minute and 5 seconds long. It depicts an adult male having penile/anal sex with a nude, pre-pubescent minor female. The male pinches the minor's labia with his fingers as he penetrates her with his penis. There are close-ups of the minor's genitals throughout and her face is visible at the end of the video. This is the same CSAM video shared on May 18, 2021.
- b. The second video is 24 seconds long. It shows an adult male having penile/anal or penile/vaginal sex with a pubescent (age difficult) female on a bed.

*Physical Surveillance & Additional Investigative Means*

31. Over the last several weeks, other investigators and myself from HSI Winston-Salem have physically surveilled 6239 Keithgayle Dr. Clemmons, North Carolina 27012, which is believed to be BROWN's primary residence. Investigators have attempted surveillance at this residence to develop a "pattern of life" for BROWN or other potential residents.

32. Although BROWN has not been physically observed at the SUBJECT PREMISES, which is the current address of record on BROWN's North Carolina Driver's License, I have personally observed a vehicle registered to BROWN, in the North Carolina Division of Motor Vehicles database with a registration address being the SUBJECT PREMISES, a white-

colored Nissan Frontier pickup (NC Registration: TDZ-4508), in the parking lot of the Honky Tonk Smokehouse located at 145 Jonestown Rd. Winston-Salem, NC 27104; additionally, on October 14, 2021, I observed a subject who appeared to be BROWN exit the same pickup just described in the parking lot of the Honky Tonk Smokehouse. After performing maintenance work on the pickup for approximately 15 minutes, the subject who appeared to be BROWN donned a baseball cap and entered the restaurant wearing what appeared to be an employee's uniform. Due to surveillance as well as law enforcement database queries, I believe this restaurant to be BROWN's primary employer; it is within a 15-minute drive from the SUBJECT PREMISES.

33. On September 30, 2021, I talked to United States Postal Service Inspector Al Sanabria. Insp. Sanabria stated that through investigative means at his disposal, he was able to ascertain that subjects with the last name of "Brown" were receiving mail at the Keithgayle Dr. residence up until the time of his inquiry. He was unable to verify which "Brown" family member(s) in particular were receiving mail at the residence currently.

34. Based on the combination of subscriber records, similarity of username & email to real-life name, and the matching cellphone numbers, I have developed probable cause regarding Cameron BROWN's involvement in this criminal activity and believe he is going to be the primary suspect for this investigation.

**HISTORIC CHILD PORNOGRAPHY OFFENSES EVOLVE TO**  
**MODERN TECH**

35. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these

materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually

explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer-to-Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, Internet Relay Chat (IRC), or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

36. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and

experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Additionally, child pornography is not “used up” as other types of contraband can be such as alcohol or drugs. Collections can be maintained on or off-site for years at a time without the “staleness” issues of other crime types. Computers, smartphones, and the



internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer (via a USB cable) or connect with a computer via Bluetooth, and transfer data files from one digital device to another. Some “smartphone” users can and do create, communicate, upload, and download child pornography, and communicate with children to coerce them or entice them to produce child pornography or perform sexual acts, by using internet based social media or electronic service providers like Instagram, Snapchat, or Apple (and many others).

d. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading

child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, LLC, Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers and is occasionally retained by the providers after the user deletes the data from their account.

f. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

g. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard

drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

h. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over terabytes of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

i. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and on the evidence of known Internet-based communications further described below, there exists a fair probability that evidence regarding the production, distribution, receipt and possession of child pornography will be found within digital devices located on the SUBJECT PREMISES and/or on the SUBJECT PERSON, or on yet-unknown digital accounts which will only be discovered through service of this search warrant and further investigation.

#### **EXPLANATION FOR SEARCH OF THE SUBJECT PERSON**

37. As technology has evolved, the digital devices utilized to access child pornography have become physically smaller and more portable. As an example, a Google search for microSD card (smaller than a nickel) brought up

digital devices capable of 512 GB of storage for \$160. This price tag is within reach of the average consumer and due to the memory card's size, could easily be concealed near-anywhere on a suspect's person. 512 GB could easily hold thousands of child pornography videos/images.

### **MANNER OF SEARCHING COMPUTER SYSTEMS**

38. As described here and in Attachment C, this application seeks permission to search for electronic devices contained within the SUBJECT PREMISES and/or on the SUBJECT PERSON for various forms of data contained therein. One form in which data may be stored is a computer's hard drive or functional-equivalent storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

39. I submit that if data is found in the electronic devices to be seized under this search warrant, there is probable cause to believe evidence of the crimes set forth in this affidavit will be located, for the reasons set forth above as well as at the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

40. As further described in Attachment C, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic, electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be stored within electronic devices located within the SUBJECT PREMISES and/or on the SUBJECT PERSON because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic

storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw



conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

41. Based on my training and experience, I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime.

The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

42. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for several reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is

impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, website, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises or a vehicle; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods,

including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

43. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password

before gaining access to the network) or “unsecured” (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator’s network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

44. Additionally, based on past investigations involving digital devices (such as cellphones), I am aware that there are significant collections of data that are potentially relevant, irrelevant, exculpatory, and/or incriminating on any digital device. Even in the case of a relatively new cellphone, initial account setup, installed telephone number, applications, storage programs, photos, videos, and other data on the device could prove to be vital to the involved investigation. Linked cloud accounts or other online identifiers could also prove vital to identifying additional off-device premises for service of new legal process for those premises’ digital contents based on the newly-identified account being associated with the digital data found inside the original

searched devices. In an age of increased interconnectivity and cloud-based computing technologies, it is possible that this service of process for the physical devices searchable under this warrant will only serve to identify and confirm additional electronic service providers where ultimately, the data resides off-site and will require another search warrant for proper access.

45. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

### CONCLUSION

46. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that Cameron James BROWN has committed these offenses. Furthermore, there is probable cause to believe that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment C, are located at 6239 Keithgayle Drive Clemmons North Carolina 27012 (the "SUBJECT PREMISES"), more specifically described in Attachment A and/or

on Cameron James BROWN ("SUBJECT PERSON"), more fully described in Attachment B. I, therefore, respectfully request that this Court issue a search warrant authorizing the search of the SUBJECT PREMISES and the SUBJECT PERSON, and the seizure of the items listed in Attachment C.

/S/ Zachary M. Neefe  
Zachary M. Neefe  
Special Agent  
Homeland Security Investigations

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which she submitted to me by reliable electronic means, on this 15<sup>th</sup> day of October, 2021, at 4:30 PM.

  
\_\_\_\_\_  
Honorable L. PATRICK AULD  
United States Magistrate Judge